UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/668,109	09/22/2003	Ram Anati	36437	7640

67801 7590 03/24/2011
MARTIN D. MOYNIHAN d/b/a PRTSI, INC.
P.O. BOX 16446
ARLINGTON, VA 22215

EXAMINER	
RAHIM, MONJUR	

ART UNIT	PAPER NUMBER
2492	

MAIL DATE	DELIVERY MODE
03/24/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/668,109	**Applicant(s)** ANATI ET AL.
	Examiner MONJOUR RAHIM	**Art Unit** 2492

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2010*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) *31-36, 42* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30,37-41 and 43-48* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *1/10/2011, 1/3/2011*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Applicant's election without traverse of 1-30, 37-41, 43-48 in the reply filed on 27 December 2010 is acknowledged.

2. Claim 31-36 and 42 withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 27 December 2010

3. Claims 1-30, 37-41, 43-48 are currently pending.

Information Disclosure Statement

4. The Information Disclosure Statement (IDS) submitted on are in compliance with the provisions of 37 CFR 1.97. Accordingly, the IDS statement is being considered by the examiner.

Priority

5. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent PCT/IL01/00758 (Israel), filed on 14 August 2001.

Drawings

6. The drawings filed on 22 September 2003 are accepted by the examiner.

Responses to the Argument

7. The applicant's arguments filed on 27 December 2010 are moot in view of new ground of rejection rendered.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-8, 11-20, 26, 30, 37-39, 41, 43-47 are rejected **35 U.S.C §102(b)** as being anticipated by Caputo et al. (US Patent No. 5878142), hereinafter Caputo.

In regard to **claim 1**, Caputo discloses:

- receiving an interaction request with said intermediate device by said intermediate device from said user (Caputo, col 5, lines 6-20), wherein user device is the one of the intermediate device which interacts with the smart card in order to authenticate the card, 19.

- responding to said interaction request by said intermediate device to said first user (Caputo, col 5, lines 7-25).

- continuing interacting with said first user by said intermediate device in response to a said authentication (Caputo, col 6, lines 43-49),

- **receiving an authentication datagram by said intermediate device, said authentication datagram including data from the user, in response to a said responding** (Caputo, col 7, lines 2-25), wherein

- protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram (Caputo, Fig 5A, col 7, lines 5-17), wherein data gets encrypted, as claimed.

- forwarding said datagram to said authentication server via the communication network, by said intermediate device, for authentication of the user (Caputo, fig 3, col 8, lines 46-55), wherein data gets sent/forwarded to security system for verification.

- **wherein said intermediate device and said authentication server are separated from one another** (Caputo, col 4, lines 20-28), wherein user terminal and authenticator are two separate entity.

In regard to **claim 2**, claim 1 is incorporated and Caputo discloses:

- **wherein said intermediate device comprises a vendor WWW site** (Caputo, Fig 3).

In regard to **claim 3**, claim 2 is incorporated and Caputo discloses:

- **wherein protecting comprises adding a signature associated with said vendor to said datagram** (Caputo, col 7, lines 43-50).

In regard to **claim 4**, claim 2 is incorporated and Caputo discloses:

- **wherein protecting comprises encrypting said datagram** (Caputo, col 6, lines 15-22).

In regard to **claim 5**, claim 1 is incorporated and Caputo discloses:

- **wherein said intermediate device comprises a user computing device** (Caputo, col 4, lines 55-59).

In regard to **claim 6**, claim 5 is incorporated and Caputo discloses:

- **wherein said computing device adds a time stamp to said datagram** (Caputo, col 8, line 59), wherein time-verifying parameter added to the data for further verification.

In regard to **claim 7**, claim 5 is incorporated and Caputo discloses:

- **wherein said computing device adds a vendor-associated information item to said datagram** (Caputo, col 7, lines 1-15), wherein unique key of the cards, inherently is the vendor-associated information.

In regard to **claim 8**, claim 5 is incorporated and Caputo discloses:

- **wherein said computing device encrypts said datagram** (Caputo, col 6, line 20).

In regard to **claim 11**, claim 5 is incorporated and Caputo discloses:

- **wherein said user computing device uses an embedded software component for said protecting** (Caputo, col 3, line 29).

I n regard to **claim 12**, claim 11 is incorporated and Caputo discloses:

- wherein said embedded software comprises an ActiveX component (Caputo, col 3, line 29).

In regard to **claim 13**, claim 11 is incorporated and Caputo discloses:

- wherein said component is cached on said user device (Caputo, Fig 4B).

In regard to **claim 14**, claim 11 is incorporated and Caputo discloses:

- wherein said component requires a property value provided by a vendor to operate (Caputo, col 6, lines 61-65).

In regard to **claim 15**, claim 1 is incorporated and Caputo discloses:

- wherein communication between said intermediate device and said server uses a secure connection (Caputo, col 4, lines 37-39).

In regard to **claim 16**, claim 1 is incorporated and Caputo discloses:

- wherein different communication paths are used for said authentication and for transaction details from said user (Caputo, Fig 3), wherein communication network used for transaction.

In regard to **claim 17**, claim 1 is incorporated and Caputo discloses:

- wherein different communication paths are used for said authentication and for transaction details from a vendor to said authentication server (Caputo, col 2, lines 31-34).

In regard to **claim 18** and Caputo discloses:

- sending an encrypted datagram by secure computer communication from vendor software to said remote authentication server, said encrypted datagram including data from the vendor (Caputo, Fig 3, col 7, lines 40-15, col 6, lines 61-65), wherein vendor specific data sent to server 38 for verification.

- receiving said encrypted datagram by said authentication server (Caputo, Fig 3).

- comparing said datagram or a hash thereof to a hash table at said server; and (Caputo, col 7, lines 49-50).

- outputting binary validation answer for authentication of the vendor (Caputo, col 8, lines 39-54).

- generating a binary validation answer by said server without an associated explanation (Caputo, col 6, lines 18-35).

- wherein said vendor software and said remote authentication server are separated from one another (Caputo, Fig 3).

In regard to **claim 19** and Caputo discloses:

- sending an encrypted datagram by computer communication from an authentication device to said remote authentication server (Caputo, Fig 4, col 8, lines 7-17).

- searching, at said server, for a hash value matching said datagram or a hash thereof, and (Caputo, col 7, liens 10-20).

- generating a validation answer by said remote authentication server, responsive to said search, wherein, said datagram includes a secret code and wherein said secret code exists only on said authentication device (Caputo, col 7, lines 8-25).

- outputting the validation answer for authentication of the first user (Caputo, col 7, lines 5-25).

- wherein said authentication device and said remote authentication server are separated from another (Caputo, col 4, lines 20-27), wherein user terminal and authenticator system are two separate entity.

In regard to **claim 20**, claim 19 is incorporated and Caputo discloses:

- wherein said authentication device includes a plurality of secret codes that are generated to appear unrelated (Caputo, col 6, lines 20-35).

In regard to **claim 26** and Caputo discloses:

- from the first user, receiving an authentication datagram by an authentication server from a remote authentication device (Caputo, col 5, lines 6-20, Fig 3), wherein user device send data to the authentication server 38.

- for each datagram received, matching said datagram or a hash of said datagram to a corresponding table (Caputo, col 7, lines 10-20).

- for each datagram received, calculating a corresponding counter value from a matching position in said corresponding table; and (Caputo, col 7, lines 10-18).

- for each datagram received, if said authentication datagram is valid, increasing said corresponding counter over a previous counter, within a certain limit (Caputo, col 7, lines 39-50).

- and for each datagram received, outputting a validation signal for the first user , in response to said corresponding counter value (Caputo, col 6, lines 20-38).

In regard to **claim 27**, claim 26 is incorporated and Caputo discloses:

- failing said authentication based on said increase being too large; and (Caputo, col 6, lines 30-40).

- allowing a subsequent authentication based on a further increase of said subsequent validation being below a second threshold(Caputo, col 7, lines 40-50).

In regard to **claim 28**, claim 27 is incorporated and Caputo discloses:

- wherein said thresholds are the same (Caputo, col 56-65).

In regard to **claim 29**, claim 27 is incorporated and Caputo discloses:

- wherein said second threshold is smaller than said certain threshold (Caputo, col 8, lines 56-65).

In regard to **claim 30**, claim 26 is incorporated and Caputo discloses:

- wherein said counter comprises an ordinal position in said table that is not apparently related to a series of generated random numbers (Caputo, col 7, lines 1-15).

In regard to claim **37**, claim 1 in incorporated:

- wherein said authentication datagram additionally includes data from a second user, wherein said forwarding includes forwarding said datagram to said authentication server for authentication of the second user (Caputo, Fig 3).

In regard to claim **38**, claim 18 is incorporated and Caputo discloses:

- wherein said encrypted datagram additionally includes data from a second user (Caputo, col 8, lines 56-67).

In regard to claim **39**, claim 19 is incorporated:

- wherein said encrypted datagram additionally includes data from a second user (Caputo, col 8, lines 56-67).

- wherein said outputting additionally includes outputting said validation answer for authentication of the second user (Caputo, col 7, lines 40-50).

.

As per claim **41**, claim 26 is incorporated:

- **wherein said method is additionally for remote validation of a second user** (Caputo, col 8, lines56-65).

- wherein said receiving additionally includes, from the second user, receiving an authentication datagram by an authentication server from a remote authentication device, wherein said receiving additionally includes, from the second user, receiving an authentication datagram by an authentication server from a remote authentication device (Caputo, Fig 3, col 6, lines 16-40).

- wherein said outputting additionally includes outputting a validation signal for the second user(Caputo, col 6, lines 20-38).

As per **claim 43**, claim 2 is incorporated:

- **carried out as part of a commercial interaction between said first user and said vendor, wherein said authentication does not require said first user to interact with a different web server** (Caputo, col 7, lines 44-55, FIG, 3).

As per **claim 44**, claim 1 is incorporated:

- wherein said receiving, protecting and forwarding is secured by a software component which is downloaded to a computing device associated with said first user and used by said user for sending an interaction request (Caputo, col 8, lines 1-15).

As per **claim 45**, claim 2 is incorporated:

- wherein said forwarded datagram includes payment instructions to said vendor (Caputo, col 5, lines 50-55).

As per **claim 46**, claim 44 is incorporated:

- wherein said forwarding comprises forwarding by said software component (Caputo, col 9, lines 5-9).

As per **claim 47**, claim 1 is incorporated:

- herein said authentication comprises a single bit authentication answer without an associated explanation (Caputo,

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in Graham **v.** John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 9, 10, 24-25 are rejected under **35 U.S.C §103(a)** as being unpatentable over Caputo and in view of Levi et al (US Patent No. 6804778), hereinafter Levi.

In regard to **claim 9**, claim 8 is incorporated:

Caputo does not explicitly teach **wherein said encryption uses a one time code**; however in a relevant art Levi teaches this function (Levi, col 7, lines 55-65).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the verification and authentication of Caputo with the encrypted one-time code disclosed in Levi since even the password get stolen by the hacker, it would not be usable to login for the second time. This provides further data security on the top of encryption. Act of using such a code out of turn will expose a non-authorized data transmission. Alternatively or additionally, since such codes cannot be reused or guessed at, they verify that a certain communication was authorized, stated by Levi at col 7, lines 60-65.

In regard to **claim 10**, claim 8 is incorporated:

Caputo does not explicitly teach **wherein said one time code is provided by a vendor for a particular session with said user;** however in a relevant art Levi teaches this function (Levi, col 7, lines 55-65).

Same motivation for combining the respective features of Caputo and Levi applies herein, as discussed in the rejection of claim 1.

In regard to **claim 2**4 and Caputo discloses:

- **receiving an authentication datagram from at least said user by a intermediate device of the vendor** (Caputo, col 5, lines 6-20), wherein user device is the one of the intermediate device which interacts with the smart card in order to authenticate the card, 19.

- **forwarding said datagram to a remote authentication server for authentication for authentication of the user when at least an indicator of said one time code that matches said**

user is provided with the said datagram (Caputo, fig 3, col 8, lines 46-55), wherein data gets sent/forwarded to security system for verification.

- **forwarding said datagram to a remote authentication server for authentication of the vendor when at least an indication of said one time code that matches the vendor is provided with said datagram; generating one time code for the user for the session** (Caputo, fig 3, col 8, lines 46-55), wherein data gets sent/forwarded to security system for verification.
- **wherein said intermediate device and said remote authentication server are separate from one another** (Caputo, fig 3), wherein user terminal and verification system are two separate entity.

Caputo does not explicitly **generating a one time code for the user for a session by a credit card**; however in a relevant art Levi teaches this function (Levi, col 7, lines 55-65).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the verification and authentication of Caputo with the encrypted one-time code disclosed in Levi since even the password get stolen by the hacker, it would not be usable to login for the second time. This provides further data security on the top of encryption. Act of using such a code out of turn will expose a non-authorized data transmission. Alternatively or additionally, since such codes cannot be reused or guessed at, they verify that a certain communication was authorized, stated by Levi at col 7, lines 60-65.

In regard to **claim 25**, claim 24 is incorporated:

Caputo does not explicitly teach **comprising signing said datagram using said one time code by said user;** however in a relevant art Levi teaches this function (Levi, col 7, lines 55-65).

Same motivation for combining the respective features of Caputo and Levi applies herein, as discussed in the rejection of claim 24.

9. **Claims 21-23, 40,** and **48** are rejected under **35 U.S.C §103(a)** as being unpatentable over Caputo and in view of Callais et al (US Patent No. 3885089), hereinafter Callais.

In regard to **claim 21** and Caputo discloses:

- A method of generating a code set for an authentication device, comprising: providing a code generating software (Caputo, col 8, lines 17-23), wherein software is inherent.

- providing at least one seed code for said software (Caputo, col 7, lines 7-10).

- generating said code set using said software and said seed (Caputo, col 8, lines 66-67 and col 9, lines 1-10).

Caputo does not explicitly teaches **destroying said seed immediately after generating said code set, and storing said code set or an indication thereof on an authentication device;** however in a relevant art Callais teaches this destroying code after using it (Callais, col 38, lines 1-12).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include the verification and authentication of Caputo with the destroying the code disclosed in Callais since it will remove any trace of the pass code . This provides further data security on the top of encryption.

In regard to **claim 22**, claim 21 is incorporated and Caputo discloses:

- comprising generating hash values for said code set (Caputo, col 7, lines 49-50).

In regard to **claim 23**, claim 22 is incorporated and Caputo discloses:

- comprising generating a second set of hash values for said code set, using a different hash function for said second set (Caputo, col 7, liens 10-20).

In regard to claim 40, claim 21 is incorporated:

wherein said remote device is additionally configured for authentication of a second user (Caputo, col 8, lines56-65).

- wherein said providing at least one seed code additionally includes providing at least one seed code for the second user for said software (Caputo, col 7, lines 7-10).

As per **claim 48**, claim 21 is incorporated:

- said code set or an indication thereof on an authentication server(Caputo, col 6, lines 20-30).

- at a later time authenticating said authenticating device by said authentication server by comparing a datagram from said authentication device against said storage at said authentication server (Caputo, col 6, lines 20-30).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Arts below, also teaches the mechanism of authentication and protecting data using encryption and signature in similar fashion.

1. US PGPUB No. 20030074569
2. US PGPUB No. 20050234826
3. US PGPUB No. 20070223725
4. US PGPUB No. 20080152137
5. US Patent No. 7765373
6. US Patent No. 3885089
7. US Patent No. 6853731

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monjour Rahim whose telephone number is (571)270-3890. The examiner can normally be reached on 7:00 AM -5:00 PM (Mo-Th).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Thomas can be reached on 571-273-6776. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (in USA or CANADA) or 571-272-1000.

/Monjour Rahim/
Patent Examiner
Art Unit: 2492
Date: 03/02/2011

/Zachary A Davis/
Primary Examiner, Art Unit 2492